Department of Commerce, Department of the Treasury, Department of Justice, Department of State, and Department of Homeland Security Quint-Seal Compliance Note:

Know Your Cargo: Reinforcing Best Practices to Ensure the Safe and Compliant Transport of Goods in Maritime and Other Forms of Transportation

OVERVIEW

Global supply chains are increasingly complex, multinational networks involving the movement of cargo by sea, freight, and air. This complexity is a consequence of the highly integrated global economy upon which our common prosperity depends. Yet such features also present opportunities for nefarious actors to evade U.S. sanctions and export control laws, including by disguising the true origin, destination, or nature of their cargo. To avoid potentially illicit conduct, individuals and entities directly participating in and enabling the global transport of goods—entities like vessel owners, charterers, exporters, managers, brokers, shipping companies, freight forwarders, commodities traders, and financial institutions—must be responsible for assessing their risk profile and implementing rigorous, risk-based internal compliance programs.

For entities involved in the maritime and other transportation industries, adherence to appropriate compliance policies and procedures will reduce the risk of sanctions and export controls violations and evasion and will help ensure secure and transparent shipping practices. This Note highlights certain tactics commonly deployed by malign actors and steps that the maritime and other transportation industries can take to ensure compliance with U.S. law.

POTENTIAL INDICATORS OF EFFORTS TO EVADE SANCTIONS AND EXPORT CONTROLS IN THE MARITIME AND OTHER TRANSPORTATION INDUSTRIES[1]

Malign actors are constantly seeking ways to exploit global supply chains for their benefit, often engaging in sanctions or export control evasion in the process. These actors frequently deploy

[1] On May 14, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the U.S. Department of State, and the U.S. Coast Guard issued a global advisory to alert the maritime industry, and those active in the energy and metals sectors, to deceptive shipping practices used to evade sanctions, with a focus on Iran, North Korea, and Syria. Companies operating in these sectors are also encouraged to review the advisory's detailed set of best practices for private industry to consider adopting to mitigate exposure to sanctions risk. *See* U.S. Department of the Treasury, U.S. Department of State, and U.S. Coast Guard, "Sanctions Advisory for the

Date: December 11, 2023

deceptive shipping or transportation practices to facilitate illicit transit of cargo connected to proscribed actors in places like Russia, Iran, and North Korea, which are subject to broad U.S. sanctions and export controls, as well as China, which remains a major transshipment point for those seeking to engage in export controls evasion. When such cargo later becomes the subject of U.S. enforcement actions (whether criminal or civil), the costs and reputational risks can be significant.

Entities operating in maritime and other transportation industries—including transportation companies, maintenance companies, insurance providers, other financial institutions, and other entities involved in funding and facilitating the transport of cargo—are therefore strongly advised to *know your cargo*, *i.e.* to institute or confirm the existence of appropriate compliance measures that protect against the following practices, especially when doing business in high-risk areas and categories of cargo:

- ***Manipulating location or identification data:*** Obfuscating the location, origin, or destination of a carrier is a common means of evading legal restrictions. For example, the Automatic Identification System (AIS) is an internationally mandated tracking system used on vessels that transmits a vessel's identification and navigational positional data, including course and speed, via high frequency radio waves. Vessels engaged in illicit trade often disable their AIS devices to mask their location and movement or manipulate their AIS data to broadcast a false location. This is often done in conjunction with the manipulation of identifiers, such as International Maritime Organization (IMO) numbers. Vessels of a certain size are required to display their name and IMO number in a visible location, and the number is intended to be permanent regardless of any change in ownership or name. In addition to false broadcasting, malign actors will sometimes paint over vessel names and IMO numbers to obscure vessel identities or pass themselves off as different vessels. Oftentimes, the use of commercial satellite imagery can assist in identifying vessels, monitoring vessel behavior, and pinpointing locations of vessels that are inconsistent with information transmitted via AIS.

- ***Falsifying cargo and vessel documents*:** Those attempting to disguise the origin or destination of their cargo may utilize falsified shipping documents, including, but not limited to, bills of lading, certificates of origin, invoices, packing lists, proof of insurance, and lists of last ports of call.

Maritime Industry, Energy and Metals Sectors, and Related Communities," (May 14, 2020), *available at* https://ofac.treasury.gov/media/37751/download?inline.

On October 12, 2023, the Price Cap Coalition issued a joint Advisory for the Maritime Oil Industry and Related Sectors concerning specific best practices in the maritime oil industry. *See* U.S. Department of the Treasury, "Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors," (Oct. 12, 2023), *available at* https://home.treasury.gov/news/press-releases/jy1797. Consistent with the May 14, 2020 Advisory and the October 12, 2023 Advisory, the guidance in this section is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law or otherwise addressing any particular requirements under applicable laws or regulations.

- ***Ship-to-ship transfers*:** Although often conducted for legitimate purposes, ship-to-ship transfers are also a tactic used in illicit maritime trade to try to conceal the origin or destination of cargo. Transfers that occur at night or in geographical areas determined to be high-risk for illicit activity are of particular concern.

- ***Voyage irregularities and use of abnormal shipping routes*:** Persons involved in illicit trade may try to disguise the destination or origin of cargo or its recipients by using indirect routing, unscheduled detours, or transit or transshipment through third countries. Such suspicious deviations in route—changes that are made without what appears to be a legitimate reason to go off-route, such as unsafe ports, extreme weather, or emergencies—may signal unlawful conduct.

- ***Frequent registration changes:*** In an effort to evade certain management measures or national provisions, those engaging in illicit maritime trade may participate in "flag hopping," which involves the repeated re-registration of the vessel under new states' flags.

- ***Complex ownership or management*:** Illicit actors take advantage of the inherent complexity of the maritime and other transportation industries by using shell companies or opaque ownership and management structures to disguise the ultimate beneficial owner of cargo, the end user, or other entities involved in the shipment process. Obscure ownership structures or frequent changes in ownership or management of companies may be a sign of illicit activity.

Individuals and entities who participate in maritime and other transportation industries should implement and strengthen compliance controls as necessary. Such controls are especially critical when operating near or in geographic areas determined to be high-risk or when dealing with counterparties who demonstrate anomalous behavior that may be indicative of deceptive shipping. A non-exhaustive list of compliance practices that may assist in identifying potential regulatory evasion efforts includes the following:

- ***Institutionalizing sanctions and export control compliance programs*:** Private sector entities should develop, implement, and adhere to written standardized, risk-based operational compliance policies, procedures, standards of conduct, and safeguards. Such compliance programs may involve communicating to business counterparties an expectation that, as industry partners, they similarly have adequate and appropriate compliance policies that respond to their internal risk assessments. Entities are strongly encouraged to use resources provided by the relevant U.S. government agencies to help develop their programs.[2]

[2] *See, e.g.*, U.S. Department of Commerce, Bureau of Industry and Security, "Export Compliance Program," *available at* https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/compliance; U.S. Department of the Treasury, Office of Foreign Assets Control, "A Framework for OFAC Compliance Commitments," *available at* https://ofac.treasury.gov/media/16331/download?inline.

- ***Establish location monitoring best practices and contractual requirements*:** Entities—particularly those of significant size and sophistication or involved in substantial transactions—are well advised to conduct risk-based due diligence on the location history of vessels, vehicles, and aircraft to identify prior manipulation or disabling of location or identification tracking data. Participants in the maritime and other transportation industries, including insurers and other financial institutions, should encourage continuous broadcasting of such data by their counterparties, and investigate signs or reports of data gaps or potential manipulation. Private sector entities should consider incorporating contractual language that prohibits any dealings restricted under U.S. laws or regulations, where appropriate.

- ***Know your customer*:** All participants in the maritime and other transportation industries, including insurers, other financial institutions, managers, and charterers, should conduct appropriate risk-based due diligence on counterparties, based on their role in a transaction. This includes screening transaction parties against government lists, such as the U.S. Government's Consolidated Screening List.[3]

- ***Exercise supply chain due diligence*:** Exporters and entities across any supply chain should conduct appropriate risk-based due diligence to ensure that recipients and counterparties to a transaction are not sending or receiving commodities in violation of U.S. sanctions or export control laws. Appropriate due diligence may include requesting copies of licenses, when applicable, and complete, accurate shipping documentation, including bills of lading that identify the origin or destination of cargo, as well as reviewing these documents to ensure that the cargo at issue was delivered to the destination identified in the documentation and not diverted. Risk-based due diligence may also involve reviewing open-source information that can be obtained through online searches and other resources.

- ***Industry information sharing*:** To help foster industry-wide awareness of challenges, threats, and risk-mitigation measures, industry groups and similar organizations are encouraged to provide members with relevant information and share it broadly with partners, other members, and colleagues. Entities should consider sharing information across industries and supply chains, as appropriate.

Where they detect any of the red flags listed above, companies are strongly encouraged to report these indications to the relevant U.S. authorities for further investigation. By reporting such concerning behaviors, industry participants can help protect their business interests,

[3] *See* International Trade Administration, "Consolidated Screening List," *available at* https://www.trade.gov/consolidated-screening-list.

international commerce, and our collective national security from malign actors and illicit conduct.

CRIMINAL AND CIVIL ENFORCEMENT ACTIONS TO COMBAT THE ILLICIT SHIPMENT OF CARGO

The Department of Justice (DOJ) can pursue civil and criminal actions to enforce U.S. laws that are violated when malign actors seek to disguise the true origins of cargo or otherwise attempt to evade U.S. sanctions and export controls. In particular, DOJ has brought multiple actions in recent years arising out of investigations into efforts by Iran to transport and sell oil products for the benefit of sanctioned Iranian entities, including the Iranian Revolutionary Guard Corps (IRGC) and the IRGC Quds Force (IRGC-QF). The IRGC, which was designated a Specially Designated National in 2007 and a Foreign Terrorist Organization in 2019, employs a network of shipping companies and front companies to illegally access the U.S. financial system and to hide their involvement in the sale and shipment of Iranian oil.[4] Proceeds from the sale of this oil are used by the IRGC to fund a full range of nefarious activities, including its proliferation of weapons, support for terrorism, and a variety of human rights abuses at home and abroad.[5] Several of the cases that DOJ has brought to combat this threat illustrate the evasion tactics described above.

In addition to partnering with DOJ on criminal investigations involving violations of the Export Administration Regulations (EAR), the Bureau of Industry and Security (BIS) can bring administrative enforcement actions, such as actions seeking significant monetary penalties and/or the denial of a company's ability to export items subject to the EAR. Primary responsibility for compliance with the EAR generally falls on the "principal parties in interest" in a transaction, who are usually the U.S. seller and the foreign buyer. Nevertheless, freight forwarders or other agents acting on behalf of the principal parties are also responsible for their actions, including the representations they make while filing export control documents. To help avoid liability in a transaction, agents and exporters must decide whether any aspect of the transaction raises red flags (such as those listed above), inquire about those red flags, and ensure that suspicious circumstances are not ignored. Failure to do so may result in penalties, as further discussed below.

The U.S. Department of State's Directorate of Defense Trade Controls (DDTC) similarly partners with DOJ in supporting criminal investigations and prosecutions. DDTC also conducts civil enforcement actions against persons who violate the International Traffic in Arms Regulations (ITAR), including imposing administrative actions, levying monetary penalties, and/or debarring a company from engaging in ITAR activities. DDTC's "ITAR Compliance Program Guidelines"

[4] U.S. Department of the Treasury, "Treasury Sanctions Iran's Largest Petrochemical Holding Group and Vast Network of Subsidiaries and Sales Agents," (June 7, 2019), *available at* https://home.treasury.gov/news/press-releases/sm703.

[5] *Id*.

outline information related to establishing a strong ITAR compliance program, including conducting compliant ITAR activities and retaining ITAR records.[6]

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) can bring civil enforcement actions against persons who violate U.S. sanctions regulations, including significant monetary penalties. All "U.S. persons"[7] must comply with U.S. sanctions, including all U.S.-incorporated entities and their foreign branches operating in the maritime and other transportation industries. Additionally, in the cases of Iran and Cuba, foreign subsidiaries owned or controlled by U.S. companies also must comply with U.S. sanctions.

Non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions. OFAC uses its enforcement discretion robustly to identify and address U.S. sanctions violations by non-U.S. persons.[8]

Criminal prosecutions

On September 8, 2023, DOJ announced the first-ever criminal resolution against a bareboat charterer of a crude oil tanker carrying contraband Iranian oil and a deferred prosecution agreement with a second company that managed the operations of the vessel during the relevant time period.[9] The two companies facilitated the sale and transport of oil from Iran, ultimately for the benefit of the IRGC and the IRGC-QF, in part through financing in the United States.[10] Specifically, they arranged for the tanker to receive oil via two ship-to-ship transfers and

[6] On December 5, 2022, and updated on September 19, 2023, the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) issued the International Traffic in Arms Regulations (ITAR) Compliance Program Guidelines. *See* U.S. Department of State, Directorate of Defense Trade Controls, "ITAR Compliance," *available at* https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_compliance_landing#sideNav. On September 11, 2023, DDTC issued a Compliance Risk Matrix for ITAR. *See id*., "ITAR Compliance Risk Matrix," *available at* https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_kb_article_page&sys_id=4f06583fdb78d300d0a370131f961913.

[7] The term "U.S. person" means any U.S. citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

[8] *See, e.g.,* U.S. Department of the Treasury, "FAQ 621," (August 6, 2018), *available at* https://ofac.treasury.gov/faqs/621; U.S. Department of the Treasury, "FAQ 1021," (March 11, 2022), *available at* https://ofac.treasury.gov/faqs/1021; U.S. Department of the Treasury, "FAQ 1029," (March 24, 2022), *available at* https://ofac.treasury.gov/faqs/1029.

[9] *See* U.S. Department of Justice, "First Criminal Corporate Resolution Involving the Illicit Sale and Transport of Iranian Oil in Violation of U.S. Sanctions," (September 8, 2023), *available at* https://www.justice.gov/opa/pr/justice-department-announces-first-criminal-resolution-involving-illicit-sale-and-transport.

[10] *Id*.

concealed the origin of the oil and that the IRGC and IRGC-QF would benefit from the transaction, causing U.S. financial institutions to be deceived and process payments in violation of U.S. law.[11]

Among the methods used to disguise the Iranian origins of the cargo were the following:

- Fabricating shipping records and vessel logs to state that the tanker received nearly 1,000,000 barrels of non-Iranian crude oil via a ship-to-ship transfer from a non-Iranian vessel when in fact it received just under 4,000 barrels from that vessel;[12]
- Engaging in a second ship-to-ship transfer of nearly 1,000,000 barrels of Iranian crude oil from another ship which was not reported on the vessel's logs;[13]
- Spoofing AIS transponder information to broadcast a false location while the vessel was loading oil;[14]
- Falsely exaggerating the tanker's depth following the transfer of oil from the non-Iranian vessel to make the tanker appear as if it were fully laden;[15]
- Falsely declaring oil transfers from the two ships as one loading operation received from the non-Iranian vessel;[16] and
- Falsely reporting the location of the vessel carrying Iranian oil during the ship-to-ship transfers to make it appear as if it were not involved in the transfer.[17]

The conduct of the bareboat charter and oil tanker operator caused a U.S. financial institution to process U.S. dollar transactions on behalf of the IRGC, thereby violating U.S. sanctions laws.[18] Following its guilty plea, the bareboat charter received a sentence of three years of corporate probation and a fine of nearly $2.5 million.[19] In addition, as a specific performance condition pursuant to its deferred prosecution agreement, the tanker operator was required to transport almost one million barrels of contraband Iranian oil across the globe to the United States at significant cost, including the loss of revenue for use of the tanker during the months-long investigation.[20] The United States then seized the nearly one million barrels of contraband crude oil on board the tanker and is pursuing a forfeiture action.[21]

---

[11] Information, *United States v. Empire Nav. Inc., et al.*, ECF No. 1, 23-CR-88 (D.D.C. 2023), ¶ 12.

[12] Statement of Offense, *United States v. Empire Nav. Inc., et al.*, ECF No. 7, 23-CR-88 (D.D.C. 2023), ¶¶ 35-37.

[13] *Id*. ¶¶ 39-46.

[14] *Id.*

[15] *Id.* ¶¶ 33-34.

[16] *Id*. ¶ 30.

[17] *Id*. ¶¶ 43-44.

[18] Information, *United States v. Empire Nav. Inc., et al.*, ECF No. 1, 23-CR-88 (D.D.C. 2023), ¶ 11(a).

[19] *See* U.S. Department of Justice, "First Criminal Corporate Resolution Involving the Illicit Sale and Transport of Iranian Oil in Violation of U.S. Sanctions," (September 8, 2023), *available at* https://www.justice.gov/opa/pr/justice-department-announces-first-criminal-resolution-involving-illicit-sale-and-transport.

[20] *Id*.

[21] United States's Verified Compl. for Forfeiture *In Rem*, ECF No. 1, *United States v. All Petroleum Product Cargo Aboard the Suez Rajan*, 23-cv-882 (D.D.C. 2023).

Civil forfeiture actions

In July 2020, DOJ filed a civil forfeiture complaint and warrant alleging that the all-petroleum product cargo aboard four different vessels was the object of a scheme to covertly ship Iranian oil via ship-to-ship transfers to Venezuela.[22] The complaint identifies several ways in which the participants sought to disguise the involvement of the IRGC and the National Iranian Oil Company (NIOC), including by

- Altering shipping documents to substitute a U.A.E.-based company as the shipper, in place of one with IRGC connections;
- Using a substitute shipper that had changed names three times in the preceding two years and had described itself as an Iranian petroleum company;
- Engaging in ship-to-ship transfers to take on Iranian oil.[23]

In October 2021, a judge with the U.S. District Court for the District of Columbia granted DOJ's motion for a default judgment forfeiting the oil to the United States.[24]

Civil enforcement actions

BIS can also impose administrative penalties for violations of the EAR related to the illicit shipment of cargo based on a strict liability standard.[25] Such penalties include monetary fines, license revocations, and prohibitions on a person's ability to export or reexport items subject to the EAR, depending on such factors as the seriousness of the violation, the culpability of the violator, and the presence of any mitigating factors.[26]

In 2018, for example, BIS imposed a civil penalty against a logistics company for exporting items to entities in China and Russia that were on one of the four proscribed parties lists administered by BIS, the Entity List. While the logistics company, acting as a freight forwarder, maintained a screening program to detect and prevent shipments to companies on the Entity List, the company used an abbreviated name for a university in China (despite knowing the full, unabbreviated name), which did not result in a "flag" in the system. In another instance, the same logistics company overrode or ignored a red flag that appeared when shipping a liquid nitrogen plant to

---

[22] *See* U.S. Department of Justice, "Warrant and Complaint Seek Seizure of All Iranian Gasoil Aboard Four Tankers Headed to Venezuela Based on Connection to IRGC," (July 2, 2020), *available at* https://www.justice.gov/opa/pr/warrant-and-complaint-seek-seizure-all-iranian-gasoil-aboard-four-tankers-headed-venezuela.

[23] United States's Verified Compl. for Forfeiture *In Rem*, ECF No. 1, *United States v. All Petroleum-Product Cargo Aboard the Bella with Int'l Maritime Org. Numb. 9208124, et al*., 20-cv-01791-JEB (D.D.C. Oct. 1, 2021), ¶¶ 19-21. Publicly-available AIS satellite tracking data showed where and when the ships were conducting their ship-to-ship transfers. *Id*. ¶ 31.

[24] *See* Mem. Op., ECF No. 35, *United States v. All Petroleum-Product Cargo Aboard the Bella with Int'l Maritime Org. Numb. 9208124, et al*., 20-cv-01791-JEB (D.D.C. Oct. 1, 2021), at 1-2.

[25] *See, e.g.*, 15 C.F.R. § 764.2.

[26] 50 U.S.C. § 4819(c)(1).

the Russian Federal Nuclear Center.[27] BIS determined that the company had "self-blinded" (*i.e.*, willingly ignored or misused information that indicated potential problems with the transactions), and imposed an administrative penalty of $155,000, of which $20,000 was suspended during a one-year probationary period.

Violations of OFAC regulations may also result in criminal or civil penalties, and OFAC has pursued civil enforcement actions against several shipping and logistics companies for violating U.S. sanctions. In 2019, for example, OFAC imposed a $871,837 civil penalty on a U.S.-based shipping company whose Chinese and Turkish subsidiaries executed agreements with third parties who had nominated blocked Iranian vessels for their shipments. The company engaged in transactions involving these blocked vessels despite knowing that financial institutions had rejected at least two earlier payments related to the vessels. [28]

Additionally, in 2022, OFAC imposed a $6,131,855 penalty against a major international freight forwarding and logistics company for causing U.S. persons to violate sanctions through the receipt of 2,958 payments related to sea, air, and rail shipments involving blocked persons on the Specially Designated Nationals and Blocked Persons List ("SDN List") and North Korea, Iran, and Syria. [29] These payments were processed through unwitting U.S. financial institutions or their foreign branches. To avoid scrutiny by these financial institutions, the company instructed its United Arab Emirates and South Korea affiliates to avoid including the names of sanctioned jurisdictions on invoices.

[27] *See* U.S. Department of Commerce, Bureau of Industry and Security, Export Enforcement, "Don't Let This Happen to You! Actual Investigations of Export Control and Antiboycott Violations," (Oct. 2022), at 35-36, *available at* https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file.

[28] *See* U.S. Department of the Treasury, "MID-SHIP Group LLC Settles Potential Civil Liability for Apparent Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations," (May 2, 2019), *available at* https://ofac.treasury.gov/media/35596/download?inline.

[29] *See* U.S. Department of the Treasury, "OFAC Settles with Toll Holdings Limited for $6,131,855 Related to Apparent Violations of Multiple Sanctions Programs," (April 25, 2022), *available at* https://ofac.treasury.gov/media/922441/download?inline.

CONCLUSION

Companies operating in the maritime and other transportation industries should be vigilant in their compliance efforts and be on the lookout for efforts to disguise the nature, origin, or destination of cargo being transported. These entities are strongly advised to assess their sanctions and export risks, implement rigorous compliance controls to address those risks and, ultimately, verify the true nature, origin, and destination of the cargo they are involved in transporting.

FREIGHT FORWARDER GUIDANCE

A freight forwarder's expertise lies in moving cargo effectively and efficiently. Members of the international forwarding community play a key role in ensuring the security of the global supply chain, stemming the flow of illegal exports, and helping to prevent weapons of mass destruction (WMD) and other sensitive goods and technologies from falling into the hands of proliferators and terrorists.

Freight forwarders should work together with exporters to ensure compliance to U.S. export controls and regulatory requirements. With respect to export controls specifically, freight forwarder roles and responsibilities are further delineated on the Department of Commerce, Bureau of Industry and Security (BIS) website: https://www.bis.doc.gov/index.php/all-articles/24-compliance-a-training/export-management-a-compliance/48-freight-forwarder-guidance.

BIS anticipates updating this guidance in the near future.